(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－115241

(43)公開日：平成９年(1997)５月２日

(51)Int.Cl.[6]	識別記号	Ｆ Ｉ	
G11B 20/10	7736-5D	G11B 20/10	H
7/00	9464-5D	7/00	Q

審査請求　未請求　請求項の数69　ＯＬ　（全16頁）

(21)出願番号　特願平8－105568

(22)出願日　平成８年(1996)４月25日

(31)優先権主張番号　特願平7－166644

(32)優先日　平７(1995)６月30日

(33)優先権主張国　日本（ＪＰ）

(31)優先権主張番号　特願平7－206085

(32)優先日　平７(1995)８月11日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　佐古　曜一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　栗原　章
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　大澤　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　弁理士　小池　晃　（外２名）

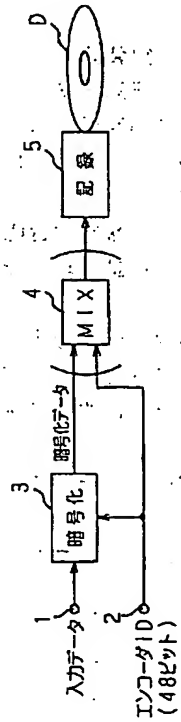
最終頁に続く

(54)【発明の名称】データ記録装置及び方法、データ再生装置及び方法、並びに記録媒体

(57)【要約】

【課題】情報が簡単に複製されることなく、また、複製されたとしても再生できない。

【解決手段】データ記録装置固有のエンコーダＩＤが入力される端子２と、少なくともエンコーダＩＤを光ディスクＤに記録する記録手段５と、端子１を介して供給される記録すべき入力データをエンコーダＩＤに基づいて暗号化する暗号化回路３とを有し、エンコーダＩＤと共に暗号化データを光ディスクＤに記録する。



1

【特許請求の範囲】

【請求項１】　記録媒体にデータを記録するデータ記録装置において、
固有の識別情報が入力される入力手段と、
少なくとも上記識別情報を記録媒体に記録する記録手段とを有することを特徴とするデータ記録装置。

【請求項２】　上記識別情報は、データ記録装置固有の識別情報であることを特徴とする請求項１記載のデータ記録装置。

【請求項３】　上記記録手段は、上記識別情報を記録媒体の所定の領域に記録することを特徴とする請求項１記載のデータ記録装置。

【請求項４】　記録媒体に記録すべきデータのデータ列に上記識別情報を混在させる混在手段を備え、
上記記録手段は、上記記録すべきデータと共に当該データ列に混在した上記識別情報を上記記録媒体に記録することを特徴とする請求項１記載のデータ記録装置。

【請求項５】　記録媒体に記録すべきデータを上記識別情報に基づいて暗号化する暗号化手段を備え、
上記記録手段は、上記識別情報と共に上記暗号化されたデータを上記記録媒体に記録することを特徴とする請求項１記載のデータ記録装置。

【請求項６】　上記記録手段は、上記識別情報を記録媒体の所定の領域に記録することを特徴とする請求項５記載のデータ記録装置。

【請求項７】　上記暗号化されたデータのデータ列に上記識別情報を混在させる混在手段を備え、
上記記録手段は、上記暗号化されたデータと共に当該データ列に混在した上記識別情報を上記記録媒体に記録するこるることを特徴とする請求項５記載のデータ記録装置。

【請求項８】　データ記録装置によって記録媒体にデータを記録する際のデータ記録方法において、
データ記録装置固有の識別情報を入力し、
少なくとも上記識別情報を記録媒体に記録することを特徴とするデータ記録方法。

【請求項９】　上記識別情報を記録媒体の所定の領域に記録することを特徴とする請求項８記載のデータ記録方法。

【請求項１０】　記録媒体に記録すべきデータのデータ列に上記識別情報を混在させて、上記記録すべきデータと共に記録することを特徴とする請求項８記載のデータ記録方法。

【請求項１１】　記録媒体に記録すべきデータを上記識別情報に基づいて暗号化し、
上記識別情報と共に上記暗号化されたデータを記録媒体に記録することを特徴とする請求項８記載のデータ記録方法。

【請求項１２】　上記識別情報を記録媒体の所定の領域に記録することを特徴とする請求項１１記載のデータ記

2

録方法。

【請求項１３】　上記暗号化されたデータのデータ列に上記識別情報を混在させ、上記暗号化されたデータと共に記録することを特徴とする請求項１１記載のデータ記録方法。

【請求項１４】　データ記録装置によってデータが記録される記録媒体において、
データ記録装置固有の識別情報を少なくとも記録してなることを特徴とする記録媒体。

【請求項１５】　所定の領域に上記識別情報を記録してなることを特徴とする請求項１４記載の記録媒体。

【請求項１６】　上記識別情報を混在したデータを記録してなることを特徴とする請求項１４記載の記録媒体。

【請求項１７】　上記識別情報と共に、当該識別情報に基づいて暗号化された暗号化データを記録してなることを特徴とする請求項１４記載の記録媒体。

【請求項１８】　所定の領域に上記識別情報を記録してなることを特徴とする請求項１７記載の記録媒体。

【請求項１９】　上記識別情報を混在した上記暗号化されたデータを記録してなることを特徴とする請求項１７記載の記録媒体。

【請求項２０】　記録データと共にデータ記録装置固有の識別情報を少なくとも記録してなる記録媒体からデータを再生するデータ再生装置であって、
上記記録媒体からデータを読み取るデータ読み取り手段と、
上記記録媒体から読み取られたデータより上記識別情報を抽出する識別情報抽出手段とを有し、
上記識別情報を抽出できないときには上記記録媒体からのデータの再生を停止することを特徴とするデータ再生装置。

【請求項２１】　上記データ読み取り手段は、記録媒体の所定の領域に記録されている上記識別情報を読み取ることを特徴とする請求項２０記載のデータ再生装置。

【請求項２２】　上記識別情報抽出手段は、上記記録媒体から読み取られたデータのデータ列に混在する上記識別情報を抽出することを特徴とする請求項２０記載のデータ再生装置。

【請求項２３】　上記識別情報に基づいて暗号化されている上記記録データの当該暗号化を、上記識別情報抽出手段により抽出した識別情報に基づいて解く暗号化解除手段を設けることを特徴とする請求項２０記載のデータ再生装置。

【請求項２４】　上記データ読み取り手段は、記録媒体の所定の領域に記録されている上記識別情報を読み取ることを特徴とする請求項２３記載のデータ再生装置。

【請求項２５】　上記識別情報抽出手段は、上記記録媒体から読み取られた上記暗号化されている記録データのデータ列に混在する上記識別情報を抽出することを特徴とする請求項２３記載のデータ再生装置。

【請求項２６】　記録データと共にデータ記録装置固有の識別情報を少なくとも記録してなる記録媒体からデータを再生するデータ再生装置であって、
上記記録媒体からデータを読み取るデータ読み取り手段と、
上記記録媒体から読み取られたデータより上記識別情報を抽出する識別情報抽出手段と、
上記識別情報に基づいて暗号化されている記録データの当該暗号化を、上記識別情報抽出手段により抽出した識別情報に基づいて解く暗号化解除手段と、を有することを特徴とするデータ再生装置。
【請求項２７】　上記データ読み取り手段は、記録媒体の所定の領域に記録されている上記識別情報を読み取ることを特徴とする請求項２６記載のデータ再生装置。
【請求項２８】　上記識別情報抽出手段は、上記記録媒体から読み取られた上記暗号化されている記録データのデータ列に混在する上記識別情報を抽出することを特徴とする請求項２７記載のデータ再生装置。
【請求項２９】　記録データと共にデータ記録装置固有の識別情報を少なくとも記録してなる記録媒体からデータを再生するデータ再生方法であって、
上記記録媒体からデータを読み取り、
上記記録媒体から読み取られたデータより上記識別情報を抽出し、
上記識別情報を抽出できないときには上記記録媒体からのデータの再生を停止することを特徴とするデータ再生方法。
【請求項３０】　記録媒体の所定の領域に記録されている上記識別情報を読み取ることを特徴とする請求項２９記載のデータ再生方法。
【請求項３１】　上記記録媒体から読み取られたデータのデータ列に混在する上記識別情報を抽出することを特徴とする請求項２９記載のデータ再生方法。
【請求項３２】　上記識別情報に基づいて暗号化されている上記記録データの当該暗号化を、上記抽出した識別情報に基づいて解くことを特徴とする請求項２９記載のデータ再生方法。
【請求項３３】　記録媒体の所定の領域に記録されている上記識別情報を読み取ることを特徴とする請求項３２記載のデータ再生方法。
【請求項３４】　上記記録媒体から読み取られた上記暗号化されている記録データのデータ列に混在する上記識別情報を抽出することを特徴とする請求項３２記載のデータ再生方法。
【請求項３５】　記録データと共にデータ記録装置固有の識別情報を少なくとも記録してなる記録媒体からデータを再生するデータ再生方法であって、
上記記録媒体からデータを読み取るデータ読み取り、
上記記録媒体から読み取られたデータより上記識別情報を抽出し、
上記識別情報に基づいて暗号化されている記録データの当該暗号化を、上記抽出した識別情報に基づいて解くことを特徴とするデータ再生方法。
【請求項３６】　記録媒体の所定の領域に記録されている上記識別情報を読み取ることを特徴とする請求項３５記載のデータ再生方法。
【請求項３７】　上記記録媒体から読み取られた上記暗号化されている記録データのデータ列に混在する上記識別情報を抽出することを特徴とする請求項３５記載のデータ再生方法。
【請求項３８】　情報提供側と情報収集側との間を結ぶ情報伝達手段と、
上記情報伝達手段を通じて情報提供側と情報収集側との間で情報を送受信するための送受信手段と、
情報提供側が情報収集側に暗号化された情報を配信するための情報媒体と、
情報収集側から送信された当該情報収集側の持つ少なくとも一つ以上の固有情報を利用して上記情報媒体の上記暗号化された情報の解読に必要な鍵情報を暗号化する鍵暗号化手段と、
情報提供側から送信された上記暗号化された鍵情報を、上記固有情報を利用して解読する暗号鍵解読手段と、
上記情報媒体の情報を読み取る情報媒体読み取り手段と、
上記解読した鍵情報を用いて、上記情報媒体から読み取った上記暗号化された情報を解読する暗号情報解読手段とを具備することを特徴とする情報提供収集装置。
【請求項３９】　上記情報提供側は、上記情報収集側から送信された、上記情報媒体を特定する媒体識別情報と、当該情報媒体内の情報を特定する情報識別情報とを用いて、課金処理を行うことを特徴とする請求項３８記載の情報提供収集装置。
【請求項４０】　上記情報収集側の持つ少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化手段を設け、
上記情報提供側に送信する上記媒体識別情報及び情報識別情報を、当該情報暗号手段により暗号化することを特徴とする請求項３９記載の情報提供収集装置。
【請求項４１】　上記情報収集側の持つ少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化手段と、
上記情報媒体から読み取った情報を蓄積する情報蓄積手段とを設け、
上記情報媒体から読み取り、上記暗号情報解読手段にて暗号を解読した情報を上記情報蓄積手段に蓄積する際には、上記暗号を解読した情報を上記情報暗号化手段にて暗号化してから蓄積することを特徴とする請求項３８記載の情報提供収集装置。
【請求項４２】　上記暗号情報解読手段は、上記固有情報に基づいて生成した鍵情報を用いて、上記情報蓄積手

段に蓄積した暗号化された情報を解読することを特徴とする請求項４１記載の情報提供収集装置。

【請求項４３】　上記情報収集側の持つ少なくとも一つ以上の固有情報は、情報媒体毎に各々異なる固有の情報を除く情報であることを特徴とする請求項３８記載の情報提供収集装置。

【請求項４４】　情報伝達手段を通じて情報提供側との間で情報を送受信するための送受信手段と、
情報提供側より配信され暗号化した情報を有してなる情報媒体から、情報を読み取る情報媒体読み取り手段と、上記送受信手段を介して送信した少なくとも一つ以上の固有情報を利用して情報提供側にて暗号化され、上記送受信手段を介して受信した鍵情報を、上記固有情報に基づいて解読する暗号鍵解読手段と、
上記解読した鍵情報を用いて、上記情報媒体から読み取った上記暗号化された情報を解読する暗号情報解読手段と、を具備することを特徴とする情報収集装置。

【請求項４５】　上記情報媒体を特定する媒体識別情報と、当該情報媒体内の情報を特定する情報識別情報とを上記情報提供側に送信することを特徴とする請求項４４記載の情報収集装置。

【請求項４６】　上記少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化手段を設け、
上記情報提供側に送信する上記媒体識別情報及び情報識別情報を、当該情報暗号手段により暗号化することを特徴とする請求項４５記載の情報収集装置。

【請求項４７】　上記少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化手段と、
上記情報媒体から読み取った情報を蓄積する情報蓄積手段とを設け、
上記情報媒体から読み取り、上記暗号情報解読手段にて暗号を解読した情報を上記情報蓄積手段に蓄積する際には、上記暗号を解読した情報を上記情報暗号化手段にて暗号化してから蓄積することを特徴とする請求項４４記載の情報収集装置。

【請求項４８】　上記暗号情報解読手段は、上記固有情報に基づいて生成した鍵情報を用いて、上記情報蓄積手段に蓄積した暗号化された情報を解読することを特徴とする請求項４７記載の情報収集装置。

【請求項４９】　上記少なくとも一つ以上の固有情報は、情報媒体毎に各々異なる固有の情報を除く情報であることを特徴とする請求項４４記載の情報収集装置。

【請求項５０】　情報伝達手段を通じて情報収集側との間で情報を送受信するための送受信手段と、
情報収集側から送信される当該情報収集側の持つ少なくとも一つ以上の固有情報を利用して、上記情報収集側に配信した暗号化された情報を有してなる情報媒体の、当該暗号化された情報の解読に必要な鍵情報を暗号化する鍵暗号化手段とを具備することを特徴とする情報提供装置。

【請求項５１】　上記情報収集側から送信されてくる上記情報媒体を特定する媒体識別情報と、当該情報媒体内の情報を特定する情報識別情報とを用いて、課金処理を行うことを特徴とする請求項５０記載の情報提供装置。

【請求項５２】　上記情報収集側の持つ少なくとも一つ以上の固有情報を用いて暗号化された上記媒体識別情報及び情報識別情報を、上記情報収集側から送信されてくる上記固有情報を用いて解読する暗号情報解読手段を備えることを特徴とする請求項５１記載の情報提供装置。

【請求項５３】　上記情報収集側の持つ少なくとも一つ以上の固有情報は、情報媒体毎に各々異なる固有の情報を除く情報であることを特徴とする請求項５０記載の情報提供装置。

【請求項５４】　情報提供側と情報収集側との間を結ぶ情報伝達工程と、
上記情報伝達工程を通じて情報提供側と情報収集側との間で情報を送受信する送受信工程と、
情報提供側により配信され暗号化した情報を有してなる情報媒体から、情報を読み取る情報媒体読み取り工程と、
情報収集側から送信された当該情報収集側の持つ少なくとも一つ以上の固有情報を利用して、上記情報媒体の上記暗号化された情報の解読に必要な鍵情報を暗号化する鍵暗号化工程と、
情報提供側から送信された上記暗号化された鍵情報を、上記固有情報を利用して解読する暗号鍵解読工程と、
上記解読した鍵情報を用いて、上記情報媒体から読み取った上記暗号化された情報を解読する暗号情報解読工程とを有することを特徴とする情報提供収集方法。

【請求項５５】　上記情報提供側は、上記情報収集側から送信された、上記情報媒体を特定する媒体識別情報と、当該情報媒体内の情報を特定する情報識別情報とを用いて、課金処理を行うことを特徴とする請求項５４記載の情報提供収集方法。

【請求項５６】　上記情報収集側の持つ少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化工程を設け、
上記情報提供側に送信する上記媒体識別情報及び情報識別情報を、当該情報暗号工程により暗号化することを特徴とする請求項５５記載の情報提供収集方法。

【請求項５７】　上記情報収集側の持つ少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化工程と、
上記情報媒体から読み取った情報を蓄積する情報蓄積工程とを設け、
上記情報媒体から読み取り、上記暗号情報解読工程にて暗号を解読した情報を上記情報蓄積工程にて蓄積する際には、上記暗号を解読した情報を上記情報暗号化工程にて暗号化してから蓄積することを特徴とする請求項５４記載の情報提供収集方法。

【請求項５８】　上記暗号情報解読工程では、上記固有情報に基づいて生成した鍵情報を用いて、上記情報蓄積工程にて蓄積した暗号化された情報を解読することを特徴とする請求項５７記載の情報提供収集方法。

【請求項５９】　上記情報収集側の持つ少なくとも一つ以上の固有情報は、情報媒体毎に各々異なる固有の情報を除く情報であることを特徴とする請求項５４記載の情報提供収集方法。

【請求項６０】　情報伝達手段を通じて情報提供側との間で情報を送受信するための送受信工程と、
情報提供側より配信され暗号化した情報が記録されてなる情報媒体から、情報を読み取る情報媒体読み取り工程と、
上記送受信工程を介して送信した少なくとも一つ以上の固有情報を利用して情報提供側にて暗号化され、上記送受信工程を介して受信した鍵情報を、上記固有情報に基づいて解読する暗号鍵解読工程と、
上記解読した鍵情報を用いて、上記情報媒体から読み取った上記暗号化された情報を解読する暗号情報解読工程と、を有することを特徴とする情報収集方法。

【請求項６１】　上記情報媒体を特定する媒体識別情報と、当該情報媒体内の情報を特定する情報識別情報とを上記情報提供側に送信することを特徴とする請求項６０記載の情報収集方法。

【請求項６２】　上記少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化工程を設け、
上記情報提供側に送信する上記媒体識別情報及び情報識別情報を、当該情報暗号工程により暗号化することを特徴とする請求項６１記載の情報収集方法。

【請求項６３】　上記少なくとも一つ以上の固有情報を用いて情報を暗号化する情報暗号化工程と、
上記情報媒体から読み取った情報を蓄積する情報蓄積工程とを設け、
上記情報媒体から読み取り、上記暗号情報解読工程にて暗号を解読した情報を上記情報蓄積工程にて蓄積する際には、上記暗号を解読した情報を上記情報暗号化工程にて暗号化してから蓄積することを特徴とする請求項６０記載の情報収集方法。

【請求項６４】　上記暗号情報解読工程では、上記固有情報に基づいて生成した鍵情報を用いて、上記情報蓄積工程にて蓄積した暗号化された情報を解読することを特徴とする請求項６３記載の情報収集方法。

【請求項６５】　上記少なくとも一つ以上の固有情報は、情報媒体毎に各々異なる固有の情報を除く情報であることを特徴とする請求項６０記載の情報収集方法。

【請求項６６】　情報伝達手段を通じて情報収集側との間で情報を送受信するための送受信工程と、
情報収集側から送信される当該情報収集側の持つ少なくとも一つ以上の固有情報を利用して、上記情報収集側に配信した暗号化された情報を有してなる情報媒体の、当該暗号化された情報の解読に必要な鍵情報を暗号化する鍵暗号化工程とを具備することを特徴とする情報提供方法。

【請求項６７】　上記情報収集側から送信されてくる上記情報媒体を特定する媒体識別情報と、当該情報媒体内の情報を特定する情報識別情報とを用いて、課金処理を行うことを特徴とする請求項６６記載の情報提供方法。

【請求項６８】　上記情報収集側の持つ少なくとも一つ以上の固有情報を用いて暗号化された上記媒体識別情報及び情報識別情報を、上記情報収集側から送信されてくる上記固有情報を用いて解読する暗号情報解読工程を備えることを特徴とする請求項６７記載の情報提供方法。

【請求項６９】　上記情報収集側の持つ少なくとも一つ以上の固有情報は、情報媒体毎に各々異なる固有の情報を除く情報であることを特徴とする請求項６６記載の情報提供方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、記録媒体にデータを記録するデータ記録装置及び方法、記録媒体に記録されているデータを再生するデータ再生装置及び方法、並びにデータが記録されてなる記録媒体に関し、また本発明は、例えばテキスト情報と共に映像や音楽等のいわゆるマルチメディア情報或いはプログラム情報を提供し、収集する情報提供／収集装置及び方法に関する。

【０００２】

【従来の技術】音声や各種データ等の情報信号が記録されるデータ記録媒体として、近年は、これら情報信号を光学的に記録するもの、具体的には音楽用のいわゆるコンパクトディスク（ＣＤ）や当該ＣＤ規格のディスクをデータ用に使用するＣＤ－ＲＯＭ等が、全世界に普及している。

【０００３】また、従来より、情報提供サービスは、例えば電話回線などを用いて利用者端末（情報収集側の端末）と情報提供者とを結び、利用者の所望する情報を取り出す、いわゆるデータベースシステムやパソコン通信システムとして実現されている。また、情報提供サービスとしては、暗号化した情報を記録したいわゆるＣＤ－ＲＯＭなどの大容量メディアを配布すると共に、上記暗号化された情報を復号するための鍵情報を例えば通信を介して利用者に送ることにより、当該ＣＤ－ＲＯＭ内に記録されている暗号化された情報を復号させ、この復号した情報をハードディスク等に複写して利用するようなサービスも出現している。

【０００４】さらに、特公平２－６０００７号公報には、ファイルキーを暗号キーで暗号化したパスワードをコンピュータに入力し、記憶媒体に書き込まれたプログラムを暗号機構で解読するようにして、ソフトウェアプログラムの複製及び共有化を防止する技術が開示されている。

【０００５】

【発明が解決しようとする課題】ところで、上述のようなＣＤやＣＤ－ＲＯＭ等に記録された情報の全てを再生装置で読み取って例えばハードディスク等にコピーし、その後、当該ハードディスクにコピーしたデータを、ＣＤやＣＤ－ＲＯＭ等のエンコーダシステムに供給して新たにＣＤやＣＤ－ＲＯＭを作成することで、元のＣＤやＣＤ－ＲＯＭと全く同じ海賊版を容易に作成することができるという具合に、従来はコピープロテクションなどのセキュリティ機能が充分ではなかった。

【０００６】また、上述の問題は、次世代のデータ記録媒体と言われているいわゆるディジタルビデオディスク（ＤＶＤ）でも深刻である。

【０００７】一方、従来の情報提供サービスの方法では、暗号を解くための鍵情報を利用者に伝送する際に、鍵情報そのものを例えば音声を使って電話で伝送するようなことが行われており、特に当該鍵情報に対する暗号化が行われることはなかった。このような鍵情報の伝送方法は、セキュリティの面から不安が大きい。

【０００８】また、鍵情報の伝送に通信を利用する場合は、通常１対１の接続なので、この鍵情報が盗まれる危険性は少ないが、鍵情報の伝送にネットワークを利用するような場合には、鍵情報の保護に問題がある。

【０００９】したがって、例えば、暗号化された情報が多量に記録されているメディアを情報提供者が配布し、利用者がこのメディアから必要な情報を所望する場合にのみ、暗号を復号するための鍵情報を伝送すると共に課金を行うような情報提供システムにおいても、上述したように鍵情報の伝送の際におけるセキュリティ面での問題があると、鍵情報が実際の利用者以外の者に知られてしまう虞れがあり、この場合、上記情報提供システム自体が成り立たなくなってしまう。また、利用者が正規の利用者かどうか特定できないと、課金が他人に行われたりしてしまう虞れもあり、やはり情報提供システムが成り立たなくなってしまう。

【００１０】このようなことから、情報提供者から利用者への鍵情報の伝送のセキュリティをいかに高めるかということ、及び利用者の特定をいかに確実に行えるようにするかとういことが重要な問題となっている。

【００１１】そこで、本発明は上述の実情に鑑み、簡単に複製されることなく、また、複製されたとしても再生できないデータ記録装置及び方法，データ再生装置及び方法、並びに記録媒体を提供するものである。

【００１２】また、本発明の他の目的は、情報提供者から利用者への鍵情報の伝送のセキュリティを高めることができると共に、利用者の特定をも確実に行うことができる情報提供／収集装置及び方法を提供することである。

【００１３】

【課題を解決するための手段】本発明のデータ記録装置及び方法は、記録媒体にデータを記録するデータ記録装置及び方法であり、固有の識別情報が入力され、少なくとも上記識別情報を記録媒体に記録することにより、上述の課題を解決する。この識別情報としては、データ記録装置固有の識別情報が挙げられる。

【００１４】また、本発明の記録媒体は、データ記録装置によってデータが記録される記録媒体であり、データ記録装置固有の識別情報を少なくとも記録してなることにより、上述の課題を解決する。

【００１５】本発明のデータ再生装置及び方法は、記録データと共にデータ記録装置固有の識別情報を少なくとも記録してなる記録媒体からデータを再生するデータ再生装置及び方法であり、上記記録媒体からデータを読み取り、上記記録媒体から読み取られたデータより上記識別情報を抽出し、上記識別情報を抽出できないときには上記記録媒体からのデータの再生を停止することにより、上述の課題を解決する。

【００１６】さらに、本発明のデータ再生装置及び方法は、記録データと共にデータ記録装置固有の識別情報を少なくとも記録してなる記録媒体からデータを再生するデータ再生装置及び方法であり、上記記録媒体からデータを読み取るデータ読み取り、上記記録媒体から読み取られたデータより上記識別情報を抽出し、上記識別情報に基づいて暗号化されている記録データの当該暗号化を、上記抽出した識別情報に基づいて解くことにより、上述の課題を解決する。

【００１７】以上の構成によれば、データ記録装置固有の識別情報を記録媒体に記録することで、この識別情報を見れば、記録媒体の作成履歴を知ることができる。また、識別情報がないときには記録媒体からのデータの再生を停止することにより、記録媒体からのデータのコピーを防止する。

【００１８】また、本発明の情報提供／収集装置及び方法は、情報収集側に暗号化された情報を有してなる情報媒体を情報提供側から配信し、情報提供側と情報収集側との間を情報伝達手段により結び、この情報伝達手段を通じて情報提供側と情報収集側とで情報を送受信し、情報提供側にて情報収集側の持つ少なくとも一つ以上の固有情報を利用して情報媒体の暗号化された情報の解読に必要な鍵情報を暗号化し、情報収集側にて情報提供側から送信された上記暗号化された鍵情報を固有情報を利用して解読し、さらに情報収集側にて上記情報媒体から読み取った暗号化された情報を上記解読した鍵情報を用いて解読することにより、上述した課題を解決する。

【００１９】すなわち、本発明によれば、暗号化された情報を有してなる記録媒体から情報を読み出す際には、当該暗号を解読するための鍵情報が必要であるが、この鍵情報は情報提供側が有しており、情報収集側はこの鍵情報の配送を要求するようにし、この際に、鍵情報の受信を受ける情報収集側から情報提供側に当該情報収集側

を特定する固有情報を送り、情報提供側は受信した固有情報から情報収集側を特定すると共に課金処理を行う。同時にこの個別情報を利用して暗号解読用の鍵情報を暗号化してから情報収集側に伝送することで、鍵情報の伝送におけるセキュリティ能力を高めるようにしている。また、情報収集側では受信した暗号化された鍵情報を固有情報により解読し、情報の解読用の鍵情報を取り出し、この鍵情報を用いて情報媒体の暗号化されている情報の解読を行う。

【００２０】

【発明の実施の形態】以下、本発明の好ましい実施の形態について、図面を参照にしながら説明する。

【００２１】本発明のデータ記録方法を実現する実施の形態のデータ記録装置は、基本構成として、図１に示すように、当該データ記録装置固有の識別情報（以下、エンコーダＩＤと呼ぶ）が入力される端子２と、少なくとも上記エンコーダＩＤを光ディスクＤに記録する記録手段５とを有するものである。

【００２２】さらに、本実施の形態のデータ記録装置においては、端子１を介して供給される記録すべき入力データを、上記エンコーダＩＤに基づいて暗号化する暗号化回路３を有し、上記エンコーダＩＤと共に上記暗号化回路３によって暗号化されたデータ（以下、暗号化データと呼ぶ）を光ディスクＤに記録するようにしている。

【００２３】なお、上記エンコーダＩＤは、上記光ディスクの所定の領域、例えば後述するＴＯＣ（table of contents）エリアやベッダ領域等に記録することができる。或いは、図１に示すように、本実施の形態のデータ記録装置の例えば記録手段５の前段にミックス回路４を設け、当該ミックス回路４において上記暗号化データのデータ列に上記エンコーダＩＤを混在させることにより、当該エンコーダＩＤを上記暗号化データが記録されるべき光ディスクＤのデータ記録領域に記録することも可能である。もちろん、記録すべきデータを暗号化しない場合も、上記ミックス回路４において記録データのデータ列にエンコーダＩＤを混在させて、光ディスクＤに記録することも可能である。

【００２４】上述のように、光ディスクＤに対してエンコーダＩＤを記録することで、当該ディスクＤにはデータ記録装置の履歴を残すことが可能となる。すなわち、データ記録装置固有の履歴を残すことができれば、例えば違法に作成されたディスクのエンコーダＩＤを見れば、いずれの装置で当該ディスクが作成されたかを知ることができる。また、このように履歴が追えることを周知させるようにすれば、ディスクをコピーすることを思いとどまらせて、違法な複製を未然に防ぐことも可能となる。

【００２５】一方、本発明のデータ再生方法が適用される実施の形態のデータ再生装置は、図２に示すように、上記本発明のデータ記録装置によって記録データと共にエンコーダＩＤが少なくとも記録されている光ディスクＤからデータを再生するものであり、上記光ディスクＤからデータを読み取るデータ読み取り手段６と、上記光ディスクＤから読み取られたデータより上記エンコーダＩＤを抽出する分離回路７とを有するものである。

【００２６】ただし、上記エンコーダＩＤが上記光ディスクの前記所定の領域に記録されているときには、上記データ読み取り手段６自身がエンコーダＩＤの抽出手段として動作し、上記記録データとは別に上記所定領域からエンコーダＩＤを読み取ることになるため、上記分離回路７は必ずしも必要ない。これに対して、上記エンコーダＩＤが記録データのデータ列に混在されているときには、上記データ読み取り手段６にて光ディスクＤのデータ領域から上記記録データとエンコーダＩＤとが共に読み出されることになるため、この場合には分離回路７にて上記記録データのデータ列からエンコーダＩＤが抽出される。

【００２７】上記記録データとエンコーダＩＤは、復号化回路８に送られることになるが、このとき、当該復号化回路８では、上記エンコーダＩＤが供給されたときには、上記記録データを再生データとして端子９から出力し、一方、エンコーダＩＤが供給されないとき（エンコーダＩＤの認証がないとき）には上記記録データの再生（復号化）を停止する。

【００２８】また、上記エンコーダＩＤと共に光ディスクＤに記録されているデータが、前記暗号化データであるとき、上記復号化回路８では、上記光ディスクＤから読み取られたエンコーダＩＤに基づいて、同じく光ディスクＤから読み取られた暗号化データの当該暗号化を解く。すなわち、これは、記録データだけをコピーできたとしても、エンコーダＩＤがなければ暗号化データの当該暗号化を解くことができないことを意味する。このようにして暗号化が解かれたデータが端子９から再生データとして取り出される。

【００２９】このように、本実施の形態のデータ再生装置によれば、記録データがコピーされたとしても、エンコーダＩＤの認証がなければ再生データを得ることができないので、セキュリティも高くなる。

【００３０】なお、前記光ディスクＤは、例えば図３に示すように、中央にセンタ孔１０２を有しており、この光ディスクＤの内周から外周に向かって、プログラム管理領域であるＴＯＣ（table of contents）エリアとなるリードイン（lead in）領域１０３と、データが記録されるデータ領域１０４と、データ終了領域、いわゆるリードアウト（lead out）領域１０５とが形成されるものである。ここで、上記エンコーダＩＤを記録データとは別の所定領域に記録する場合には、例えばリードイン領域１０３等のデータ領域１０４以外の領域に記録することになる。また、記録データに混在させてエンコーダＩＤを記録する場合には、データ領域１０４に記録され

ることになる。

【００３１】また、前述した実施の形態におけるデータ記録装置としては、例えばオーディオデータやビデオデータ、或いはプログラムデータ等に誤り訂正符号を付加したり変調したりするエンコーダ或いはフォーマッタや、いわゆるカッティング装置、マスタリング装置、スタンピング装置等が考えられ、上記エンコーダＩＤはこれら装置固有の識別情報となる。さらに、光ディスクＤが光磁気ディスク（ＭＯディスク）や、レコーダブルのＣＤ（いわゆるＣＤ－Ｒ）である場合、上記エンコーダＩＤはこれらディスクの記録再生装置固有の識別情報となる。

【００３２】次に、上述した光ディスクＤを再生するデータ再生装置の概略構成について、図４を用いて説明する。この図４の説明では、記録データがエンコーダＩＤに基づいて暗号化されており、さらに当該エンコーダＩＤが暗号化データのデータ列に混在されて記録されている場合の動作について述べる。

【００３３】この図４において、光ピックアップ１７は、上記光ディスクＤ上にレーザ光を集光し、このレーザ光の反射光を受光することにより、当該光ディスクＤに記録されているデータ信号を読み出し、このデータ信号をデコード回路１５に送る。また、光ピックアップ１７は、上記レーザ光の反射光に基づくフォーカスサーボエラー信号，トラッキングエラー信号をサーボ回路１４に送る。

【００３４】サーボ回路１４は、コントローラＣＰＵ１０の制御に基づき、上記フォーカスサーボエラー信号，トラッキングエラー信号に応じたフォーカスサーボ信号及びトラッキングサーボ信号を生成して光ピックアップ１７に送る。また、当該サーボ回路１４からは、光ディスクＤの回転サーボ信号も出力され、モータ１８は当該回転サーボ信号により回転が制御される。

【００３５】一方、デコード回路１５では、上記光ピックアップ１７からのデータ信号の復調及び誤り訂正処理を行う。

【００３６】ここで、上記光ディスクＤのデータ記録領域１０４から読み出され、上記デコード回路１５によりデコードされたデータは、先ず、例えばセクタ単位でエンコーダＩＤ抽出回路１９に送られる。当該エンコーダＩＤ抽出回路１９は、上記セクタ単位のデータから、上記エンコーダＩＤのデータを抽出する。この抽出されたエンコーダＩＤのデータは、コントローラＣＰＵ１０により制御されるワークＲＡＭ１２に蓄えられる。

【００３７】このとき、コントロールＣＰＵ１０は、上記エンコーダＩＤのデータが抽出された残りの暗号化データを、上記ＲＡＭ１２に蓄えられたエンコーダＩＤのデータを用いて復号化する。なお、上記コントローラＣＰＵ１０が使用するプログラムデータはプログラムＲＯＭ１３に蓄えられている。

【００３８】上述のようにして復号化された再生データは、インターフェイス回路１６を介して出力端子１１から外部に出力される。

【００３９】上記図４のデータ再生装置における動作の流れは図５に示すようなものとなる。

【００４０】この図５において、ステップＳ１で光ディスクＤの読み取りが開始されると、次のステップＳ２では光ディスクＤからセクタ毎にデータが読み出される。

【００４１】次のステップＳ３では、前記エンコーダＩＤ抽出回路１９により、当該セクタ毎のデータからエンコーダＩＤのデータが抽出される。

【００４２】ステップＳ４では上記エンコーダＩＤのデータが抽出された残りの暗号化データを読み出し、ステップＳ５ではコントロールＣＰＵ１０にて上記暗号化データをエンコーダＩＤに基づいて復号化する。

【００４３】その後、ステップＳ６では、上記復号化したデータを再生データとしてインターフェイス回路１６に送る。

【００４４】次のステップＳ７では、光ディスクＤの再生が終了したか否かの判定を行い、いまだ再生が終了していないと判定したときにはステップＳ１に戻って上述の処理を行い、再生が終了したときには処理を終了する。

【００４５】次に、本発明に係る情報提供及び／又は収集方法の実施の形態について、図面を参照しながら説明する。

【００４６】本発明の情報提供／収集方法が適用される情報提供／収集装置、すなわち情報提供システムとしては、図６に示すように、情報収集側の利用者端末４００と情報提供者側の情報提供装置２００とが、情報伝達手段としての電話回線やローカルエリアネットワーク（ＬＡＮ）などの通信網３００によって結ばれた状況を想定している。

【００４７】ここで、上記情報提供システムにおける情報提供装置２００は、図７に示すように、利用者側に送出する情報及び当該送出情報を暗号化するための鍵情報を蓄積する情報蓄積装置２０１と、利用者毎の課金情報及び利用者の電話番号及び利用者の固有番号の情報を蓄積する情報蓄積装置２０２と、送出情報を上記鍵情報に基づいて暗号化する暗号化回路２０３と、送出情報を回線に送出できるように変換する変換器２０４と、通信網（通信回線）３００に情報を送出するための通信回線インターフェイス部２０６と、当該装置２００の制御プログラム及びシステムの構成情報を記憶したＲＯＭ２０９と、上記制御プログラムを実行するＣＰＵ２０７と、ＣＰＵ２０７の一時的な作業情報を記憶しておくためのＲＡＭ２０８と、データバス，アドレスバス，制御バスなどよりなるＣＰＵ２０７のシステムバス２１０とから構成されている。

【００４８】また、利用者端末４００の構成は、図８に

示すように、一時的に情報を記憶しておくＲＡＭ４１１と、例えばハードディスクや光磁気ディスク等の少なくとも情報を保存しておくことができる情報蓄積装置４１２と、情報蓄積装置４１２から読み出した情報を表示するための表示信号を生成する表示回路４１３と、表示回路４１３からの表示信号に基づいた表示を行う表示装置４１４と、当該端末４００を操作するための例えばキーボードやマウス等の操作装置４１５と、情報提供装置２００からの暗号化情報を解読する暗号解読回路４１６と、情報提供者により配布された情報記録媒体を読み出す情報媒体読み取り装置４１７と、情報媒体読み取り装置４１７固有の識別番号（ＩＤ）情報を保持するＲＯＭ４１８と、当該端末４００の制御プログラム及び端末４００の構成情報を記憶したＲＯＭ４２０と、制御プログラムを実行するＣＰＵ４１９と、通信網（通信回線）３００に情報を送出するための通信回線インターフェイス部４２１と、データバス，アドレスバス，制御バスなどよりなるＣＰＵ４１９のシステムバス４２２とから構成されている。

【００４９】以下に、上述した情報提供装置２００と通信網３００と利用者端末４００とからなる情報提供システムの動作について、利用者側と情報提供者側との間の通信網３００（通信回線）として例えばいわゆるＩＳＤＮ（サービス総合ディジタル網）の回線を利用した場合について説明する。

【００５０】利用者は、先ず始めに情報提供者が無償或いは有償で配布する大容量の情報蓄積媒体３０１を入手する。なお、上記情報蓄積媒体３０１は、例えば光記録媒体であるいわゆるＣＤ－ＲＯＭなどの大容量の情報蓄積メディアを使用しており、多量の暗号化された情報が記録されている。その他、当該ＣＤ－ＲＯＭのような読み出し専用の媒体以外に、ライトワンス或いは光磁気ディスクのような記録可能な媒体を使用することも可能である。またこのとき、当該利用者端末４００の読み出し専用メモリのＲＯＭ４１８には情報読み取り装置４１７の固有の識別番号（以下読み取り装置ＩＤと呼ぶ）が記録されており、情報蓄積媒体３０１には当該媒体を識別するためのＩＤ（以下媒体識別ＩＤと呼ぶ）及び当該媒体３０１内の各々の情報を識別するためにＩＤ（以下情報識別ＩＤと呼ぶ）が記録されている。さらに、利用者は個別のＩＤ（以下利用者ＩＤと呼ぶ）及びパスワードを持つ。

【００５１】このような前提の元、利用者が所望の情報を上記情報蓄積媒体３０１から読み出す場合の手順を図９～図１２を用いて詳細に説明する。

【００５２】図９のＡの部分には、利用者端末４００から情報提供装置２００側に送出する情報を記述してある。すなわち、利用者端末４００から送出する情報は、利用者の固有の番号情報であり、例えば、電話発番号、利用者ＩＤ、パスワード、読み取り装置ＩＤ及び情報の特定に必要な媒体識別ＩＤ、情報識別ＩＤからなる。電話発番号は、利用者の電話番号であり、ＩＳＤＮでは発信者から着信者に向けて電話番号を（発番号）を自動的に送ることができるようになっている。

【００５３】先ず、図１０を用いて、利用者端末４００での動作から説明する。

【００５４】この図１０において、利用者端末４００のＣＰＵ４１９は、ステップＳ５０１にて情報記録媒体３０１が当該端末４００の情報媒体読み取り装置４１７にセットされたか否かの判断を行う。当該ステップＳ５０１で情報記録媒体３０１がセットされていないと判断した場合にはこのステップＳ５０１の判断を繰り返し、セットされたと判断した場合にはステップＳ５０２に進む。なお、情報記録媒体３０１を読み取る情報媒体読み取り装置４１７は、当該情報記録媒体３０１が着脱可能なものである。

【００５５】次に、利用者は、端末４００の操作装置４１５を操作することにより、情報蓄積媒体３０１内の所望の情報の検索処理を行う。このときのＣＰＵ４１９は、操作装置４１５からの目次情報表示の指示があるか否かの判定を行い、無いと判定した場合にはステップＳ５０２の判定を繰り返し、有ると判定した場合にはステップＳ５０３に進む。ステップＳ５０３では、利用者による操作装置４１５の操作に応じて、端末４００の情報媒体読み取り装置４１７にセットした情報記録媒体３０１から目次情報を再生し、この再生された目次情報に基づく表示信号を表示回路４１３が生成し、この表示信号を表示装置４１４に送ることで表示画面上に上記目次情報が表示される。なお、上記目次情報には、上記情報蓄積媒体３０１内に記録されている情報の一部内容の閲覧が可能なものも含まれる。

【００５６】次のステップＳ５０４では、ＣＰＵ４１９が上記表示装置４１４の表示画面上に表示された目次情報の内から上記操作装置４１５の操作による検索操作がなされているか否かの判断を行い、無いと判断した場合にはステップＳ５０４の判断を繰り返し、有ると判断したときにはステップＳ５０５に進む。このステップＳ５０５では検索中の内容表示が行われる。ステップＳ５０６では、ＣＰＵ４１９において上記検索表示された内容の内の何れかに対して、利用者から操作装置４１５を介して情報を取り出す指示が入力されたか否かの判断を行う。このステップＳ５０６にて取りだし指示がなされていないと判断したときにはステップＳ５０５に戻り、指示されたと判断したときにはステップＳ５０７に進む。このステップＳ５０７では指定された情報のＩＤ情報の読み取りを行う。すなわち、ステップＳ５０４～ステップＳ５０７までの検索操作においては、利用者が希望する情報を見つけることができたとき、利用者が上記操作装置４１５を操作することにより、情報蓄積媒体３０１からその内容を取り出す指示が行われ、当該指示入力が

有ったときにはその指定した情報のＩＤ情報を該当する情報蓄積媒体３０１から読み取る。

【００５７】次のステップＳ５０８では、情報媒体ＩＤを同様にして情報蓄積媒体３０１から読み取り、ステップＳ５０９に進む。

【００５８】このステップＳ５０９では、ＣＰＵ４１９が情報提供者に発呼処理を行う。すなわち、予め設定されている情報提供者の電話番号を情報蓄積装置４１２から読み出し、通信回線インターフェイス部４２１に設定する。このとき、ステップＳ５１０のように、当該通信回線インターフェイス部４２１は情報提供者の情報提供装置２００に発呼動作を行い回線を接続する。

【００５９】次のステップＳ５１１では、ＣＰＵ４１９が情報提供装置２００に送り出す情報を準備し、ステップＳ５１２に進む。ここで、上記情報提供装置２００に送り出す情報は、情報媒体ＩＤ、情報識別ＩＤ、利用者ＩＤ、パスワード、情報媒体読み取り装置ＩＤである。ステップＳ５１２では、ＣＰＵ４１９において、これらのうち情報媒体ＩＤと情報識別ＩＤ、情報媒体読み取り装置ＩＤに対して、利用者ＩＤとパスワードを用いて暗号化処理を行う。

【００６０】その後、ステップＳ５１３において、暗号化された情報は、通信回線インターフェイス部２１を介して情報提供者の情報提供装置２００に送られ、ステップＳ５１４にて情報提供装置２００からの送信待ち状態となる。

【００６１】次に、情報提供者側の処理について説明する。すなわち、図９のＢの部分に記述するように、利用者端末４００からの発呼があると、情報提供装置２００は、媒体識別ＩＤと情報識別ＩＤとから利用者の必要とする情報を特定し、該当する解読鍵情報を、読み取り装置ＩＤ、利用者ＩＤ、パスワード、電話番号を利用して暗号化して利用者端末４００に送信する。

【００６２】この処理動作を図１１を用いて説明すると、ステップＳ５３０では、ＣＰＵ７は先ず利用者端末４００からの送信（発呼）が有るか否かの判断を行っており、無いと判断した場合には待ち状態としてステップＳ５３０の判断を繰り返している。このステップＳ５３０において、有ると判断した場合にはステップＳ５３１に進む。このステップＳ５３１では、ＣＰＵ２０７が、上記利用者端末４００から通信回線を通って供給された前記暗号化された情報を、通信回線インターフェイス部２０６、変換器２０４を介して読み込む。

【００６３】次のステップＳ５３２において、ＣＰＵ２０７は、受信した利用者ＩＤを元に、情報蓄積装置２０２に保存している利用者の課金情報の中にあるパスワードを読み出し、利用者ＩＤと組み合わせて、受信した暗号化情報の解読を行う。次のステップＳ５３３では、上記ステップＳ５３２での解読の結果、読み出された情報媒体ＩＤと情報識別ＩＤを使って、情報蓄積装置２０１に蓄積されている情報媒体管理情報から該当する情報の解読鍵情報を得る。

【００６４】ステップＳ５３４では、上記得られた解読鍵情報を、利用者ＩＤ、パスワード、読み取り装置ＩＤと共に暗号化回路２０３に送り、ここで暗号化を施した後、ステップＳ５３５にて、変換器２０４、通信回線インターフェイス部２０６を経て、利用者端末４００に送る。すなわち、図９のＣに示すように、情報提供装置２００から利用者端末４００に送られる情報は、暗号化された解読鍵情報である。

【００６５】次に、上記情報提供装置２００からの暗号化された解読鍵情報を受信した利用者端末４００では、図１２に示す処理を行う。すなわち、当該暗号化された解読鍵情報を受信した利用者端末４００では、図９のＤに示すように、固有番号を使って、上記暗号化された解読鍵情報を解読し、この解読した解読鍵情報を利用して情報蓄積媒体３０１上の暗号化されている情報を解読する。

【００６６】図１２において、前記ステップＳ５１４のように情報提供装置２００からの送信待ち状態となっている利用者端末４００では、ステップＳ５１５にて情報提供装置２００からの送信が有ったか否かの判断を行っており、送信が無いときにはこの判断を繰り返し、送信が有ったならばステップＳ５１６の処理を行う。

【００６７】ステップＳ５１６では、ＣＰＵ４１９が上記通信回線インターフェイス部４２１を通して受信した上記暗号化された解読鍵情報を暗号解読回路４１６に送る。

【００６８】当該暗号解読回路４１６では、ステップＳ５１７に示すように、利用者ＩＤ、パスワード、情報媒体読み取り装置４１７の固有番号である読み取り装置ＩＤを、ＲＯＭ４１８から受け取り、これらを用いて上記受信した暗号化された解読鍵情報の解読を行う。

【００６９】次のステップＳ５１８では、上述のようにして暗号解読回路４１６にて解読された解読鍵情報を用いて、ＣＰＵ４１９が情報蓄積媒体３０１に記録されている、暗号化されている所望の情報を読み出させ、暗号解読回路４１６に送る。暗号解読回路４１６では、上記暗号化されている所望の情報の暗号を上記解読鍵情報を用いて解読し、利用者が利用可能な平文情報を得る。

【００７０】ステップＳ５１９では、上記平文情報を表示回路４１３に送り、当該表示回路４１３にて生成された上記平文情報の表示信号を表示装置４１４に送る。これにより、表示装置４１４の表示画面上には、利用者が読み取ることができる形の上記平文情報の表示がなされる。

【００７１】なお、上述の説明では、表示装置４１４の表示画面上に平文情報を表示するまでについて述べているが、上記平文化情報を情報蓄積装置４１２に複写する場合には、当該平文化情報をそのまま情報蓄積装置４１

19

２に複写することは行わず、当該平文化情報を前記ＣＰＵ４１９にて情報媒体読み取り装置のＩＤと利用者のＩＤにより暗号化してから蓄積記録するものとする。この情報蓄積装置４１２に蓄積した情報を読み出す場合には、情報蓄積装置４１２からの上記暗号化された情報を、暗号解読回路４１６に送り、ここで情報媒体読み取り装置ＩＤと利用者ＩＤを元に情報の解読を行うようにする。また、本構成例では、情報提供者の情報提供装置２００と利用者端末４００との間を接続する情報伝達手段としてＩＳＤＮ回線を用いた例を説明したが、通常のアナログ電話回線やＣＡＴＶ回線（ケーブルテレビジョン回線）、無線通信回線、ＬＡＮ（ローカルエリアネットワーク）等を利用した場合も容易に実現可能であることは言うまでもなく、さらには通信回線ではなく郵便や宅配便にて情報の受け渡しを行う場合であっても、本発明は適用できる。

【００７２】さらに、上述の例では、利用者の個別の識別情報として利用者ＩＤやパスワードを用いているが、この利用者個別の識別情報としては、利用者端末４００の機器番号や、利用者の電話番号、利用者の定めた暗証番号、ネットワークインターフェイスの物理アドレス等を用いることもできる。なお、利用者端末４００の機器番号を上記個別の識別情報として用いた場合、暗号解読回路４１６に当該機器番号情報が直接供給されるように構成することも可能である。

【００７３】上述したように、本発明にかかる情報提供システムによれば、多量の情報を大容量の情報記録媒体に纏めて記録したものを利用者に配布し、通信回線やネットワーク等を介して所望の情報についての暗号を解読するための解読鍵情報を伝送するシステムを構築した場合、読み取り装置に固有の番号（ＩＤ）にて暗号化した解読鍵情報を情報提供者側から送信するようにすることで、解読鍵情報を万一回線やネットワークから傍受されたとしても、当該傍受者は正しい解読鍵情報を得ることが不可能となるので、セキュリティ能力を向上することが可能となる。

【００７４】また、利用者端末から、情報読み取り装置のＩＤ等の利用者固有のＩＤ情報を暗号化して情報提供装置側に送り、それを元にして情報提供装置側では解読鍵情報を暗号化してから利用者端末側に送るようにしていることも、セキュリティの面から有効である。

【００７５】さらに、情報媒体読み取り装置から他の情報蓄積装置に情報を複写する際にも、必ず読み取り装置のＩＤを使って暗号化してから書き込むようにしているので、違法コピーの防止をすることが可能となる。ここで、読み取り装置のＩＤは利用者から操作や読み取りが不可能な形で構成することで、さらにセキュリティ能力を高めることが可能である。すなわち、情報蓄積媒体から読み出した情報を利用者端末において複製する場合には、一度暗号を解読した情報をそのまま複製することも

20

可能であるが、本発明の構成例では、上述したように、一度解読した情報を再度情報読み取り装置のＩＤ情報の複数の固有情報で暗号化し直すことで、よりセキュリティ能力を高めるようにしている。

【００７６】なお、米国特許第５，３９２，３５１号の電子化データ保護方式にて示されるように、情報媒体に予め一意の媒体固有番号と共に暗号化した暗号化電子化データを書き込んでおき、許諾側で媒体の一意の媒体固有番号を元に媒体固有鍵を生成し、この媒体固有鍵によって暗号化電子化データ復号鍵を暗号化し、この暗号化したデータを媒体に許諾情報として書き込み、使用側で媒体から読み込んだ媒体固有番号を元に媒体固有鍵を生成し、媒体から読み込んだ許諾情報をこの媒体固有鍵によって復号して元の電子化データ復号鍵を生成し、この電子化データ復号鍵によって媒体から読み込んだ暗号化電子化データを復号し、平文の電子化データを生成するようなものも存在している。しかし、このような情報媒体毎にそれぞれ異なるの固有のＩＤ（例えば媒体固有のシリアルナンバ等）を前提にして電子化データ復号鍵を生成するものの場合、ＣＤ－ＲＯＭのように大量複製される媒体にそれぞれに固有のＩＤ情報を記録することは困難である。これに対して、本発明にかかる情報提供システムにおいては、情報蓄積媒体の媒体識別ＩＤはそれぞれの媒体毎に固有のＩＤである必要はなく、媒体内に記録されている情報も各々の媒体で同一の暗号化処理が行われたものにできるため、大量複製が可能となり、したがってＣＤ－ＲＯＭのような媒体に適用可能である。さらに、上記電子化データ保護方式では、許諾側が電子化データ復号鍵を暗号化し、この暗号化した電子化データ復号鍵を許諾情報として媒体に書き込んでから、使用者側に使用させるようにしているので、このことからも上記ＣＤ－ＲＯＭのように大量複製される媒体には不向きであるのに対して、本発明では、解読鍵情報の伝送の際に、利用者から情報読み取り装置ＩＤなど利用者固有のＩＤを情報提供側に通信回線を介して送出し、情報提供側ではそれを元に解読鍵情報を暗号化して再び通信回線を介して利用者に送り返すようにしているため、大量複製される媒体であっても有効に適用できる。上述のようなことから、本発明によれば、情報記録媒体の製造時に固有の情報を記録しなくてもよいため、製造コストが上昇することなく、安価に製造できることになる。

【００７７】

【発明の効果】本発明においては、データ記録装置固有の識別情報を記録媒体に記録することで、この識別情報を見れば、記録媒体の作成履歴を知ることができ、このことから簡単に複製が行われることを防止できる。また、識別情報がないときには記録媒体からのデータの再生を停止することにより、記録媒体からのデータのコピーを防止できる。

【００７８】また本発明においては、情報収集側に暗号

21

化された情報を有してなる情報媒体を情報提供側から配信し、情報提供側と情報収集側との間を情報伝達手段により結び、この情報伝達手段を通じて情報提供側と情報収集側とで情報を送受信し、情報提供側にて情報収集側の持つ少なくとも一つ以上の固有情報を利用して情報媒体の暗号化された情報の解読に必要な鍵情報を暗号化し、情報収集側にて情報提供側から送信された上記暗号化された鍵情報を固有情報を利用して解読し、さらに情報収集側にて上記情報媒体から読み取った暗号化された情報を上記解読した鍵情報を用いて解読することにより、情報提供側から情報収集側への鍵情報の伝送のセキュリティを高めることができると共に、情報収集側の特定をも確実に行うことができる。

【図面の簡単な説明】

【図１】本発明に係る実施の形態のデータ記録装置の基本構成を説明するための図である。

【図２】本発明に係る実施の形態のデータ再生装置の基本構成を説明するための図である。

【図３】本実施の形態の光ディスクの構成について説明するための図である。

【図４】本実施の形態の光ディスクを再生するデータ再生装置の具体的構成を示すブロック回路図である。

【図５】本実施の形態の光ディスクからのデータ再生時の動作の流れを示すフローチャートである。

【図６】本発明にかかる情報提供システムの構成例を示すブロック回路図である。

【図７】情報提供システムの情報提供装置の構成例を示

22

すブロック回路図である。

【図８】情報提供システムの利用者端末の構成例を示すブロック回路図である。

【図９】情報提供システムでの動作及び伝送される情報について説明するための図である。

【図１０】利用者端末から情報提供装置へ暗号化情報を送信するまでの処理の流れを示すフローチャートである。

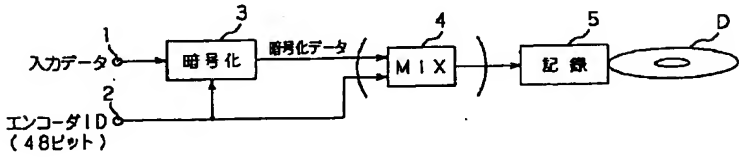
【図１１】情報提供装置から利用者端末へ暗号化した解読鍵情報を送信するまでの処理の流れを示すフローチャートである。

【図１２】情報提供装置からの暗号化された解読鍵情報を用いて、情報蓄積媒体の暗号化された情報を解読するまでの利用者端末における処理の流れを示すフローチャートである。

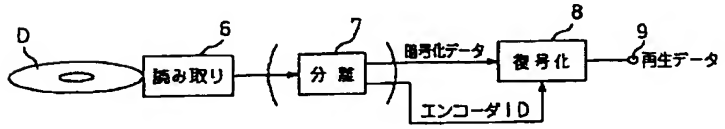
【符号の説明】

３　暗号化回路、　４　ミックス回路、　５　記録手段、　６　データ読み取り手段、　７　分離回路、　８　復号化回路、　Ｄ　光ディスク、　２０１，２０２，４１２　情報蓄積装置、　２０３　暗号化回路、　２０６，４２１　通信回線インターフェイス部、　２００　情報提供装置、　２０７，４１９　ＣＰＵ、　３００　通信網、　３０１　情報蓄積媒体、　４００　利用者端末、　４１３　表示回路、　４１４　表示装置、　４１５　操作装置、　４１６　暗号解読回路、　４１７　情報媒体読み取り装置

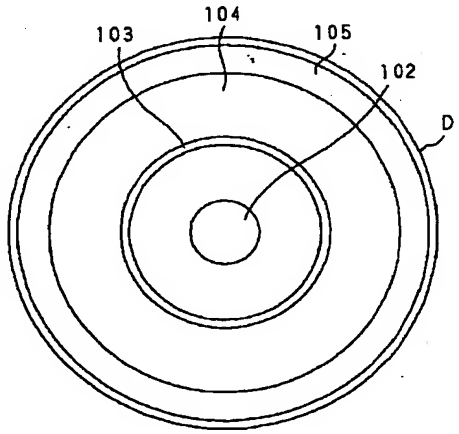
【図１】



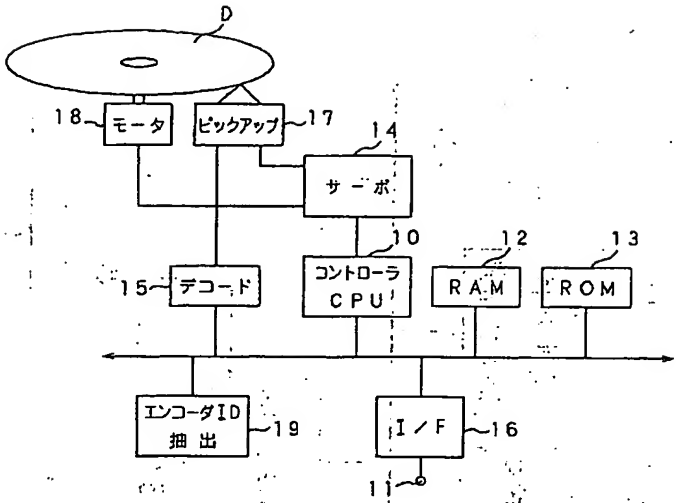
【図２】



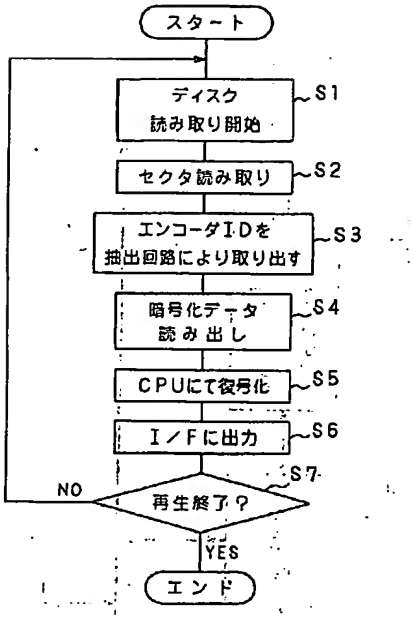
【図３】



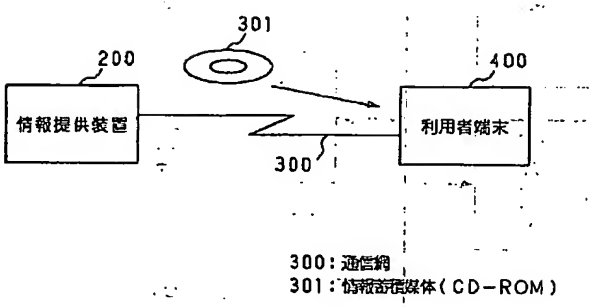
【図４】


D
18
モータ
ピックアップ
17
14
サーボ
10
コントローラ CPU
12
RAM
13
ROM
15
デコード
エンコーダID 抽出
19
I／F
16
11

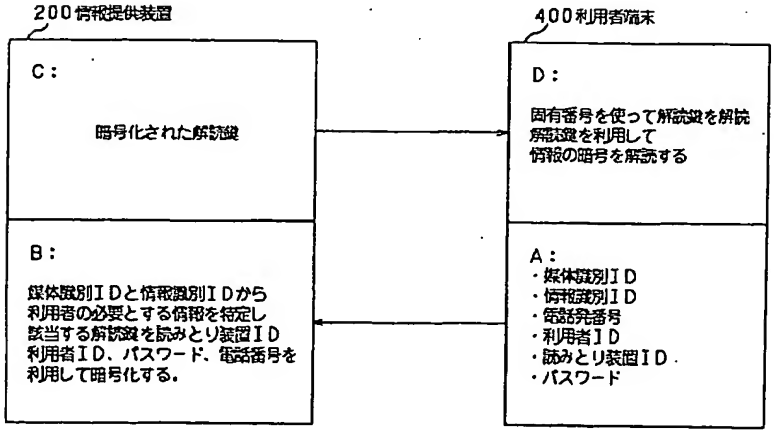
【図５】


スタート
ディスク 読み取り開始
S1
セクタ読み取り
S2
エンコーダIDを 抽出回路により取り出す
S3
暗号化データ 読み出し
S4
CPUにて復号化
S5
I／Fに出力
S6
再生終了？
S7
NO
YES
エンド

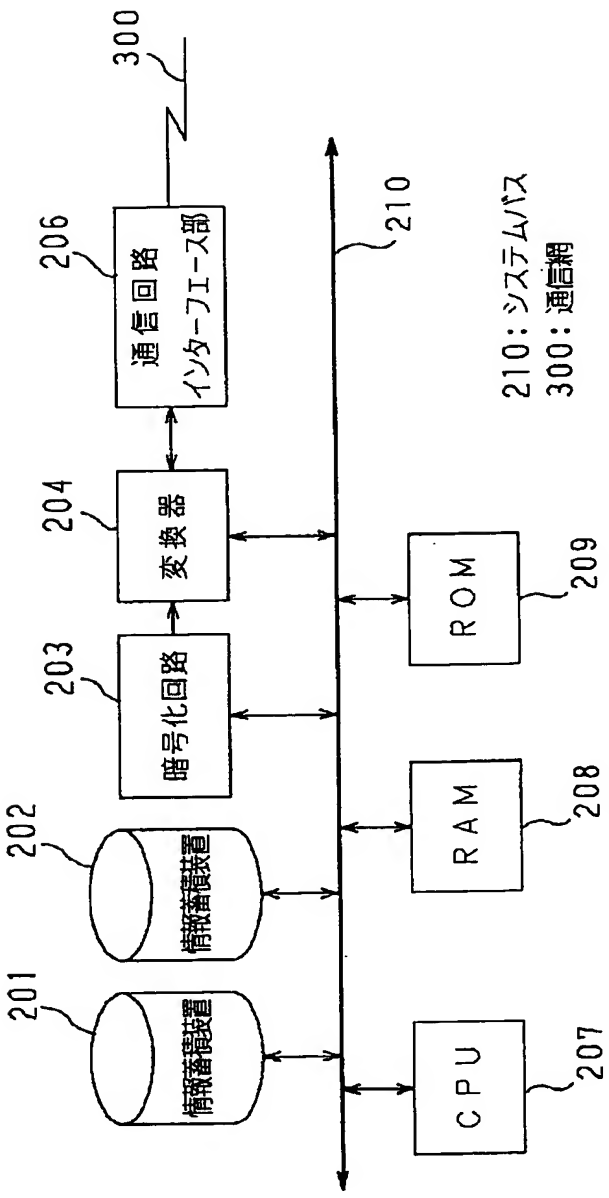
【図６】


301
200
400
情報提供装置
利用者端末
300
300：通信網
301：情報記録媒体（CD－ROM）

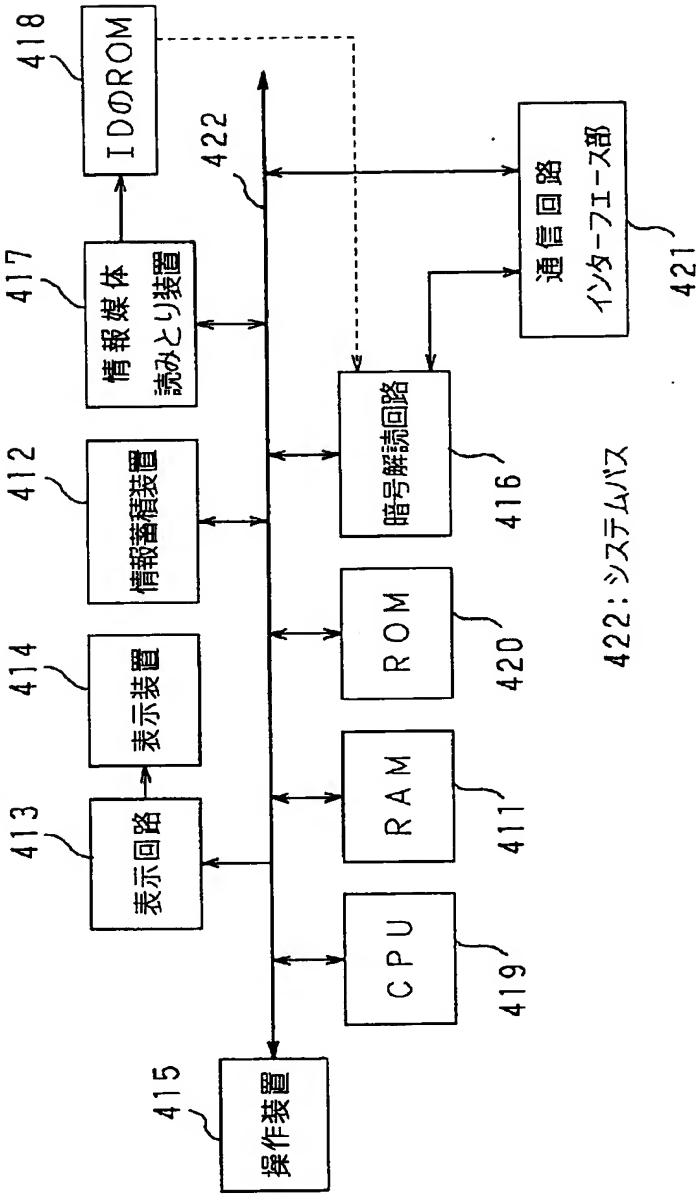
【図９】


200情報提供装置
400利用者端末
C：
暗号化された解読鍵
D：
固有番号を使って解読鍵を解読
解読鍵を利用して
情報の暗号を解読する
B：
媒体識別ＩＤと情報識別ＩＤから
利用者の必要とする情報を特定し
該当する解読鍵を読みとり装置ＩＤ
利用者ＩＤ、パスワード、電話番号を
利用して暗号化する。
A：
・媒体識別ＩＤ
・情報識別ＩＤ
・電話発番号
・利用者ＩＤ
・読みとり装置ＩＤ
・パスワード

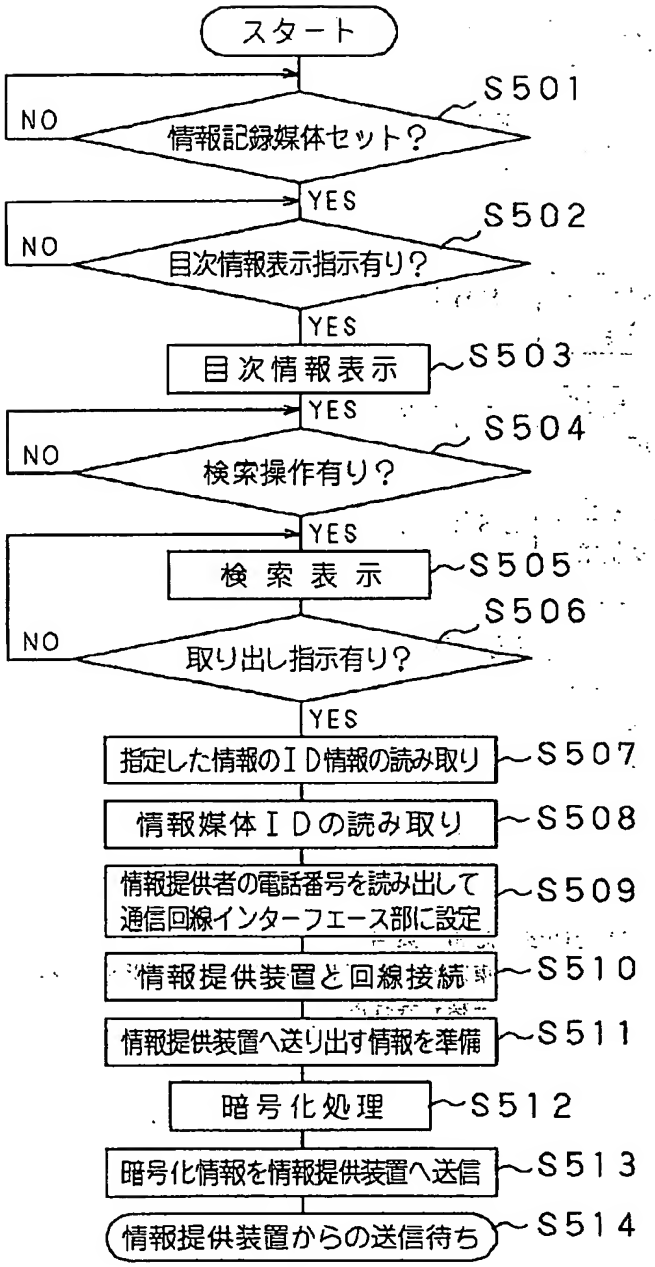
【図7】


300
通信回路
インターフェース部
206
210
204
変換器
203
暗号化回路
202
情報蓄積装置
201
情報蓄積装置
ROM
209
RAM
208
CPU
207
210：システムバス
300：通信網

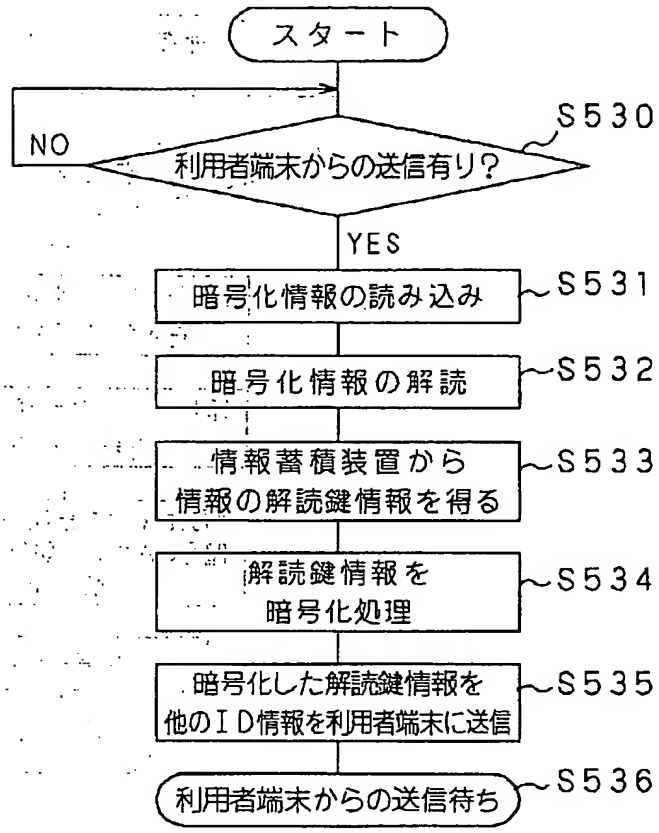
【図8】


418
IDのROM
422
通信回路
インターフェース部
421
417
情報媒体
読みとり装置
412
情報蓄積装置
暗号解読回路
416
414
表示装置
ROM
420
413
表示回路
RAM
411
CPU
419
415
操作装置
422：システムバス

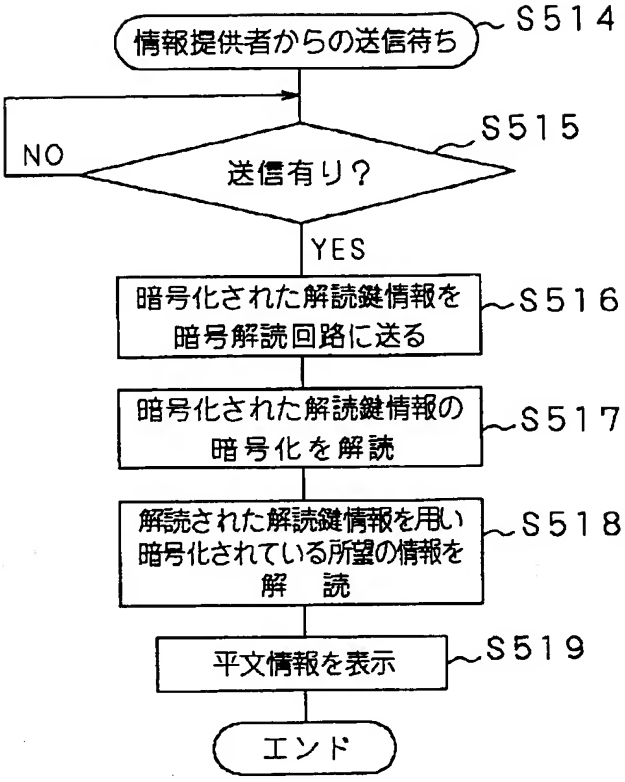
【図１０】


スタート
S501
NO
情報記録媒体セット？
YES
S502
NO
目次情報表示指示有り？
YES
目次情報表示
S503
YES
S504
NO
検索操作有り？
YES
検索表示
S505
S506
NO
取り出し指示有り？
YES
指定した情報のＩＤ情報の読み取り
S507
情報媒体ＩＤの読み取り
S508
情報提供者の電話番号を読み出して
通信回線インターフェース部に設定
S509
情報提供装置と回線接続
S510
情報提供装置へ送り出す情報を準備
S511
暗号化処理
S512
暗号化情報を情報提供装置へ送信
S513
情報提供装置からの送信待ち
S514

【図１１】


スタート
S530
NO
利用者端末からの送信有り？
YES
暗号化情報の読み込み
S531
暗号化情報の解読
S532
情報蓄積装置から
情報の解読鍵情報を得る
S533
解読鍵情報を
暗号化処理
S534
暗号化した解読鍵情報を
他のＩＤ情報を利用者端末に送信
S535
利用者端末からの送信待ち
S536

【図１２】



フロントページの続き

(72) 発明者　川嶋　功
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72) 発明者　応和　英男
東京都品川区北品川６丁目７番35号　ソニー株式会社内